CITY OF CHICOPEE, MASSACHUSETTS

PERSONAL INFORMATION PROCEDURE/POLICY

It is the policy of the City of Chicopee that all information be treated as confidential and personal. All departments have a responsibility to develop processes and follow all policies and procedures required for the protection of confidential information.

From 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth:

"Personal information," a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"Record" or "Records," any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

1. Every department shall appoint at least one employee that shall serve as the designated liaison, or "information security officer", in implementing and monitoring these regulations. Each department shall forward the appropriate information designating such person to Human Resources and ensure that all information regarding the designee is current. At no time shall a department fail to have in place an employee to monitor the handling of confidential or personal information.

2. Every department shall be mindful of possible risks to the security, confidentiality and/or integrity of any electronic, paper or other records containing personal information. It shall be the duty of each department to identify all risks, alert Human Resources, and remedy them within a timely manner.

3. All personal information that is transported outside of the business premises must be stored in a sealed, opaque envelope or container. The envelope or container may not be left unattended at any time. When possible, the department's information security officer shall be notified of the transport of all confidential information outside of the business premises.

4. Any personal or confidential information that is disposed of must be passed through a paper shredder so that all information stored on the document is no longer readable or

recoverable. Each department will have at least one paper shredder in an area easily accessible to all employees.

5. Disciplinary actions for violations of this policy will be handled on an individual basis, but may include the suspension and termination of any violating employee.

6. All departments shall notify Human Resources and Management Information Systems when an employee is terminated, transferred, retires or resigns. When possible, the department shall notify Human Resources and Management Information Systems prior to the end of employment. If it is not possible to give notice before the end of employment, the department must alert Human Resources and Management Information Systems immediately after notice has been given to the employee.

7. All departments shall maintain and keep current a list of all third party vendors, businesses, people or organizations that have access to files within their department.

8. All departments shall maintain a written policy in maintaining and safeguarding information available to third party vendors, businesses, people or organizations. Every third party entity that has access to personal information must provide the City of Chicopee with a written, comprehensive information security program that is in compliance with 201 CMR 17.00 and this policy.

9. Any requests for verification of personal information for an employee must be made in writing and accompanied with a release form signed by the employee to release the designated information to the requesting party. The formal request should have the contact information of the entity requesting the information for verification purposes.

10. All collected information shall be limited to that reasonably necessary to accomplish the legitimate purpose for which it is collected.

11. All electronic devices, such as laptops, flash drives or disks that contain personal information shall be treated as if it were an actual document and in accordance with these guidelines.

12. All personal or confidential files shall be stored in a locked container. Keys to those containers shall be stored in a responsible and responsible manner. It is recommended that containers be stored in a locked facility or storage area away from public access. All storage containers shall be locked when not in use. Exceptions may apply with approval from Human Resources.

13. Human Resources shall conduct random audits and inspections of departments that store personal information.

14. This policy shall be revised and updated on an annual basis. Human Resources will distribute a survey on an annual basis requesting ways in which this policy can be improved and the intent of this policy advanced.

15. All breaches of security shall be documented and forwarded to Human Resources. A post-incident review will be conducted by the Director of Human Resources to determine how the breach occurred, disciplinary action, changes in business practice and future security compliance.

16. Changes to this policy or requests for non-compliance shall be made to Human Resources in a written request and granted only by written permission from the Director of Human Resources.

17. All electronic information shall be stored in a manner that restricts access to records and files containing personal information.

18. All usernames and passwords shall be unique to each user and shall not be default usernames or passwords provided by the hardware or software manufacturer. All passwords shall be stored in a location and/or format that do not compromise the security of the data they protect.

19. No employee shall allow their passwords to become compromised at any time for any reason.

20. Employees shall be trained and educated on the proper use of computer security protocols and the importance of securing electronic data.

21. Any system that connects to the internet shall have a reasonably up-to-date firewall and virus protection program operating at all times.

22. All programs that require a user to log-in must be exited when not in use or when the employee leaves the computer for any amount of time.

23. All employees must follow the guidelines set forth in the "Acceptable Use of City Technology Resources" maintained by M.I.S. For a copy of the policy, please contact Human Resources or M.I.S.

Effective: April 15, 2009